IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 0:22-cv-00098-WMW-JFD

SECOND EXPERT DECLARATION OF BENJAMIN R. COTTON

December 12, 2024

I, Ben Cotton hereby declare and state as follows:

I) I am over the age of 18, and I understand and believe in the obligations of an oath. I make this declaration of my own free will and based on first-hand information and my own personal observations.

2) I am submitting this declaration as a supplemental declaration to my declaration dated September 22, 2023 and as a rebuttal to the declaration submitted by Dr. Alan T. Sherman for Plaintiffs' Motion for Partial Summary Judgment.

3) I have over twenty-seven (27) years of experience performing computer forensics and other digital systems analysis, including the detection and analysis of intrusions, malware analysis and root cause analysis of intrusions.

4) I have over nineteen (19) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software. These courses included network intrusion investigations.

5) I have regularly lead engagements involving digital forensics, investigations to detect security breaches, discover malware and cyber security investigations for law firms, corporations, and government agencies. I am experienced with the digital acquisition of evidence under the Federal Rules of Evidence.

6) While serving as Vice President of Incident Response for eSentire, USA and using software that I developed, my team investigated three to five system breaches per week worldwide including for companies in the United States and foreign companies overseas.

7) An example of my practical experience in forensics in the real world may be helpful. On April 22, 2015 I detected malware that resided in the Office of Personnel Management (OPM) with software that I had created. This malware had resided in multiple servers and systems for

over three (3) years without detection and was the cause of the largest breach in US Government history, approximately 22.1 million records. Donna Seymour, who was the Chief Information Officer for OPM, acknowledged my discovery of this malware in a televised congressional hearing before the House Committee on Government Oversight and Reform shortly before her resignation.[1]

8) In the course of my duties, I have forensically examined voting systems in Maricopa County Arizona, Antrim County Michigan, Mesa County Colorado, Coffee County Georgia, and Adams Township, Michigan. In the course of Antrim County examinations I examined a Dominion ImageCast X (ICX). The Dominion ICX is a ballot marking device that performs similar functions to the Smartmatic equipment used in LA County, California.

9) In the course of my duties, I have reviewed available public information from the Election Assistance Commission (EAC) regarding voting system certification status and the certification process for election software. In the course of this review, I determined that Smartmatic currently does not have any active certifications by the EAC for any of their voting systems. The EAC certified election systems can be found at the following link: https://eac.gov/voting-equipment/certified-voting-systems. There are no systems or components from Semantic that are certified by the EAC.

10) I have reviewed the Opening Expert Report of Alan T. Sherman, PH.D. dated September 21, 2023.

11) I have reviewed the "Dr. Alan T. Sherman's Rebuttal Report of Micheal Lindell and My Pillow's Expert Declaration of Benjamin R. Cotton" dated 9 July 2024.

[1] Chaffetz, Jason (September 7, 2016). "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation"

12) I have reviewed the Plaintiff's inspection protocol titled " INSPECTION PROTOCOL FOR MODEL VSAP BMD IN OCTOBER 2023"

13) In the course of this legal proceeding the Plaintiff's offered to permit the inspection of a representative Smartmatic BMD150 ballot marking device. This is the same model that was inspected by Dr. Alan Sherman. However, it is important to note that the plaintiffs did not indicate that the device offered for inspection would even be the same device inspected by Dr. Sherman, only that it would be the same model.

14) Furthermore, the offered device was not used in the 2020 elections, nor would it have been configured by LA County personnel to perform as a component of the VSAP voting system.

15) Paragraph H of the protocol stated "With the exception of the removal of the ballot box, Defendants' inspection of the BMD shall **exclude** any physical tampering with the BMD, including but not limited to removing any hardware coverings to expose the inside of any part of the BMD; removing the tablet/touch screen from the frame; or removing the thermal printer."

16) Under the guise of preventing tampering, the Plaintiffs prevented any effective forensic preservation of the software for analysis or physical inspection of the tablet/touchscreen. These preventative measures would have prevented any inspection of the motherboard for embedded components such as 802.11 Wi-Fi wireless modems, Bluetooth capability, additional storage mechanisms and/or additional communications capabilities. To inspect this device under these conditions would have been a waste of time with respect to proving or disproving the legal claims asserted by the Plaintiffs.

17) It is clear that, despite Plaintiffs' representations to the contrary, the model BMD150 they offered for inspection is not the model that was utilized by LA County in the 2020 elections. Paragraph 4.2.2 on page 31 of the VSAP Use Procedures manual dated June 19, 2020 states that the approved BMD is model number BMD100. I am shocked that Dr. Sherman did not note this discrepancy. Once again to simply examine a BMD150 that was not used or even the same model that was used in the LA County elections would not have been relevant to proving or disproving the facts of this litigation.

18) To date I have not been offered the opportunity to properly examine a Smartmatic BMD or analyze any forensic image of a Smartmatic BMD that was configured and used in the LA County election. It is baffling to me that any expert could positively assert that something did not occur without a forensic examination of the systems involved. Based on my experience with other litigations involving digital devices, I do not believe that the Plaintiffs preserved the digital evidence necessary to prove the facts in this litigation.

19) In my twenty-seven (27) years of performing intrusion and breached systems investigations I have never heard of any legitimate expert claiming to be able to determine whether the memory, software and/or operating system of a given system was breached by simply looking at the external computer case of a system and relying on manuals. Seals and other devices affixed to the computer case simply notify an investigator if that case was accessed or opened, but in no way will determine if the software is modified, malware is injected into the active memory or the system is misconfigured.

20) Dr. Sherman attempted to analogize his conclusion to the metaphor of a bridge that remains standing. Quite frankly, I cannot understand the analogy because it has nothing to do

with determining a breach. A more appropriate example is setting out four identical voting machines where one is known to have a breach and intrusion. If one were to merely walk around and examine the exterior of all four machines one would not be able to point out which one was breached by visual inspection alone. Yet like the bridge, the four machines are still there—but so is the breach.

21) In all but one engagement that I performed the systems were remotely compromised and exploited. In situations involving remote access, the status of the screws, USB ports and other physical indicators on the computer were irrelevant to the determination if the software, databases, or operating systems were compromised. In the one examination that was a result of local physical access, the insider threat actor did utilize the USB port on the system to modify the internal software and operating system of the compromised computer. It is beyond credulity that anyone could examine a BMD that was not used in the 2020 LA County elections, examine a model number of the BMD that was not authorized for use in the VSAP system, and examine a BMD that was not configured for use in the VSAP system by simply walking around the system then declare that the election was the safest and most secure election in U.S. history.

22) In every engagement that I have conducted, a forensic analysis and analytical process was required to determine 1) if the system was breached or compromised, 2) the type of compromise that occurred, and 3) extent to which the compromise affected the data and processes of the compromised system. It is my expert opinion rendered to a high degree of professional certainty that it is simply impossible to determine if a system or network is compromised without this analysis.

23) In the Incident Response engagements that I have conducted the findings have determined that often misconfigured systems, user error, and failure to follow sound cyber security principles were key elements of the breach. As part of the investigative process, the personnel who are responsible for the security of the systems are interviewed. In almost all cases these individuals indicated that their systems are secure. The findings of the examinations, however, lay bare the truth that their systems were not secure. To simply accept a statement from an administrator or officer of a company that their systems are secure is not an effective or responsible means to determine the security posture of a system or to determine if the system has been breached.

24) At the time that operating systems (OS) such as, but not limited to, Windows, Linux Variations, Unix, iOS, Android, and Apple OSX are released there are inevitably vulnerabilities that are unknown to the producers of the operating systems that allow for remote access by unauthorized parties. Limited versions of operating system modifications are especially prone to possess vulnerabilities. There is not an operating system currently in existence that does not possess these vulnerabilities. To determine if these vulnerabilities were exploited on a specific device or set of devices would require the forensic acquisition of the device and the analysis of the device to determine the extent of the exploitation.

25) In computing processes such as the Smartmatic BMD performs it is necessary to store data and values in memory as part of that process. For example, when a voter chooses the candidates as part of the voting process those choices would be stored in volatile memory while the QR code is created and the voter's paper ballot is sent to the printer. Smartmatic has issued multiple statements that the BMD does not store the voter's choices on disk. This situation creates the possibility that if an unauthorized individual could inject malware that

was capable of scraping memory for data, that data could be changed prior to it being printed for review. It is important to note that while part of the printed ballot is human readable, the QR code is not human readable and requires the knowledge and proper technology to review what is actually recorded in the QR code. Such memory scraping and modification malware is routinely used in stealing credit card information and could easily be adapted to steal and modify voter data.

26) The claim that there has never been a case where a voting system flipped votes or incorrectly tabulated votes is false. The claim that there has never been an election where the voting systems flipped votes and caused a determinative error in the result of the election is false.

a) On May 24, 2022 in the DeKalb County, GA primary election for county commissioner the electronic voting system determined the District 2 County Commission race was won by Marshall Orson, with 5,226 votes. Candidate Lauren Alexander was determined by the electronic voting system to have received 4,382 votes, Candidate Michelle Long Spears was determined to have received 3,031 votes and Candidate Donald Broussard was determined to not have received a single vote. Note that the total number of votes according to the electronic election system was 12,639 votes. There were no flags or warnings by the election equipment that anything was amiss. The results were challenged by Candidate Donald Broussard as both he and his wife had voted for him. A hand recount revealed that there were actually 15,449 votes cast and Michelle Long Spears had actually won the election with 6,651 votes. Auditors concluded that the machines incorrectly scanning and tabulating the ballots. Votes that were meant for one candidate were being allocated to other

candidates.[2] [3] [4] This instance was clearly a 'flipping' of the votes that resulted in an incorrect outcome of the election. The root cause of this flipping was centered in the election data file that was used by the election systems during the tabulation of the election results.

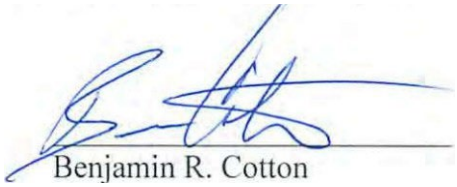
b) On November 3, 2020 in Antrim County Michigan during the 2020 General Election, the electronic voting systems mis-allocated, i..e. "flipped", votes between the presidential candidates. Initially the voting systems had Candidate Joe Biden winning the County by over 3,000 votes. The county clerk felt the results did not 'look' right and initiated a 100% hand recount. This recount determined that Candidate Trump had actually won the county with 9,748 votes. Analysis of this issue by the county and state indicated that there was an error with the election definitions and election database. The fact that the database and definition issues were not flagged by the voting software is a significant issue with the voting software and the system testing procedures.

c) During a local election in Williamson County, Tennessee on October 26, 2021 the electronic voting system incorrectly designated legitimate cast ballots as provisional ballots, marked those ballots as provisional ballots and did not include those ballots in the initial vote results and tabulation. An investigation by the EAC determined that the root cause of this issue was erroneous code contained in the source code of the scanner software.[5]

[2] Dominion Botch: Georgia Primary Election Overturned After Awful Machine Count - League of Power;,
[3] Botched vote count in DeKalb race caused by Georgia programming mistake, May 27, 2022
[4] Georgia Candidate Who Appeared to Get Few Votes Was Actually in 1st Place - The New York Times, June 6, 2022
[5] EAC Issues Report on Tennessee Voting System Anomaly | U.S. Election Assistance Commission, April 1, 2022.

I declare under penalty of perjury under the laws of the United Sates of America that the foregoing is true and correct.

Executed on 12 December 2024



Benjamin R. Cotton